трактування персоналу підприємства. З позиції логіко-змістовного підходу щодо розуміння даної категорії, а також комплексного та системного підходів, автор пропонує наступне визначення персоналу: персонал підприємства – особовий склад кваліфікованих робітників підприємства, фірми або організації, які володіють професійною здатністю до праці, тобто мають спеціальну підготовку та потребують грамотного управління і створення умов для їхнього розвитку, а також здатні до змін відповідно до розвитку інших факторів і елементів виробництва.

Список літератури: **1**. *Покривний С. Ф.* Економіка підприємства. – К.:Либідь, 2005. – 238 с. **2.** *Маслов А. В.* Управління персоналом підприємства. –К.: Либідь, 2007. –187 с. **3.** *Шокін К.К.* Основи кадрового менеджменту. – К.: Либідь, 2006. –345 с.

СТРОКОВ Є.М., к.е.н., доц., каф ЕАтаО НТУ «ХПІ»

ЩОДО ПОБУДОВИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В певний період свого існування будь-яка організація, незалежно від видів її діяльності, або від форми власності, стикається з необхідністю забезпечення конфіденційності внутрішньої інформації. Таким чином, можна вважати, що інформаційна безпека організації - це стан захищеності інформаційного середовища організації, що забезпечує його формування, використання й розвиток.

Оскільки в основі успішного функціонування кожної організації полягають дані, що є основою її діяльності, її комерційною таємницею. Це може бути база даних покупців і постачальників, бухгалтерські та управлінські документи, ділова переписка, інформація про технології, ноу-хау, персональні дані співробітників і багато чого іншого. Втрата або розголошення цієї інформації може призвести до негативних наслідків для компанії. Система інформаційної безпеки покликана попереджати такий розвиток подій.

Система інформаційної безпеки – це набір засобів, методів та робіт, спрямованих на захист інформаційної інфраструктури підприємства від будь-яких зовнішніх або внутрішніх загроз, що можуть привести до крадіжки, пошкодження або несанкціонованій зміні даних на серверах або робочих станціях. Всі роботи, що орієнтовані на побудову, підтримку та розвиток системи мають у підґрунті одну ціль – мінімізувати можливість нанесення шкоди інформаційній інфраструктурі підприємства, а у випадку форс-мажорних обставин – зведення до мінімуму такої шкоди.

Для забезпечення інформаційної безпеки перш за все необхідно визначити найбільш імовірні канали витоку інформації, засобу їх контролю, а, при необхідності, і перекриття. Для цього слугує аудит інформаційної безпеки. Аудит дозволяє виявити канали витоку, оцінити їх критичність та ймовірність витоку по них. Аналіз даних, зібраних під час аудиту, дає можливість вибору засобів контролю каналів. Аудит передбачає:

- Аудит системи інформаційної безпеки;
- Аудит програмного забезпечення;
- Аудит інформаційної системи.

Наступним кроком забезпечення інформаційної безпеки є побудова або оновлення та модернізація окремих напрямків системи інформаційної безпеки:

- Захист від вторгнень;
- Захист файлів і документів від несанкціонованого доступу;
- Захист клієнт-банку;
- Єдина система аутентифікації та дистанційний доступ до всіх ресурсів компанії;
- Оптимізація й захист 1С;
- Захист корпоративних комунікацій;
- Контроль роботи персоналу;
- Забезпечення стабільності та безперервності бізнес-процесів;
- Екстрене знищення інформації.

І ще один важливий крок – побудова системи фізичної безпеки з використанням технічних засобів:

- Система відеоспостереження;
- Система контролю і управління доступом;
- Система оповіщення;
- Домофони.

Такий комплексний підхід до побудови системи інформаційної безпеки має забезпечити максимально можливу ступінь захисту корпоративної інформації.

ШЕЛЕСТ Т.М., ст. викладач, м. Київ, КДАВТ

СТЕЙКХОЛДЕР-МЕНЕДЖМЕНТ В СИСТЕМІ ПІДГОТОВКИ МОРЯКІВ

Не дивлячись на скорочення українського флоту в десятки разів, найбільш перспективним для України напрямком праці у морській діяльності залишився ринок підготовки моряків. На сьогоднішній день Україна входить в п'ятірку країн світу, які постачають моряків “під прапор” по командному складу і в десятку країн світу – по рядовому складу. Основну підготовку моряків забезпечують ВМНЗ, проте фінансування на придбання новітнього тренажерного обладнання практично не здійснюється. Тому виникає гостра необхідність у пошуку додаткових джерел залучення коштів на ці потреби. Одним з нових інструментів залучення коштів на підготовку моряків є впровадження інструментів стейкхолдер-менеджменту в діяльність ВМНЗ.

Основне визначення даного поняття дав Н. Е. Фріман (R.E. Freeman) в 1984 році: «Стейкхолдер — це група (індивід), яка може вплинути на досягнення організацією своїх цілей або на роботу організації в цілому». Отже, стейкхолдери — це всі групи людей (або інших організацій), чий внесок (праця, капітал, ресурси, купівельна спроможність, поширення інформації про компанії тощо) створює підґрунтя для розвитку та успіху організації.

В наукових колах існують різні підходи до класифікації стейкхолдерів. За ступенем впливу їх поділяють на первинних та вторинних. Первинні стейкхолдери - це суб’єкти, що надають вирішальний вплив на діяльність компанії (споживачі, кредитори, партнери). Вторинні стейкхолдери – це групи субєктів, взаємний вплив яких знаходиться в прямій або непрямій залежності від діяльності або рішень зацікавленого підприємства (держава, місцеві органи, суспільство, співтовариства, ЗМІ). Вчені Ньюбоулд і Луффман (1989) поділяють стейкхолдерів на чотири групи: групи впливу, які фінансують організацію (держава, акціонери), менеджерська група,